京都大学学術情報リポジトリ
KURENAI 紅
Kyoto University Research Information Repository

京都大学
KYOTO UNIVERSITY

Title	On some infinite totally real extensions of $ \mathbb{Q}$(Definable sets in various fields)
Author(s)	Fukuzaki, Kenji
Citation	数理解析研究所講究録 (2007), 1574: 1-21
Issue Date	2007-11
URL	http://hdl.handle.net/2433/81333
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

Kyoto University

数理解析研究所講究録
第1574巻 2007年 1-21

On some infinite totally real extensions of $\mathbb{Q}$

鹿児島国際大学国際文化学部　福崎賢治 (Kenji Fukuzaki)
Faculty of Intercultural Studies,
The international University of Kagoshima

Abstract

Every number fields are known to be undecidable. Nevertheless the only known undecidable infinite algebraic extensions of the rationals are fields whose descriptions depend on non-recursive sets. No 'natural' such fields seem to be known until now.

Let l be a prime greater than 5 and $l \equiv -1 \pmod 4$. We prove that a subset A of K_l such that $\mathbb{Z} \subsetneq A \subsetneq \mathfrak{O}_{k_l}$ is definable in the ring language using the formula of Julia Robinson in [8] and give some propert-es of A, aiming to prove the undecidability of $K_l = \bigcup_n \mathbb{Q}(\cos(2\pi/l^n))$.

1 Introduction

In 1959 Julia Robinson [8] proved that any number field, as well as the corresponding ring of algebraic integers, is undecidable, by showing that $\mathbb{N}$ is $\emptyset$-definable (in the ring language) in the ring, and the ring is $\emptyset$-definable in its number field. The formulas which she used depend on number fields. Later she [9] showed that there is a uniform way of defining $\mathbb{N}$ in the ring of algebraic integers of a number field. Hence, the theory of the ring of algebraic integers of number fields is undecidable.

These results were extended by R. Rumely [12] to prove that the theory of global fields is undecidable. His formula is independent of global fields. (J. Robinson used the Hasse-Minkowski theorem on quadratic forms. On the other hand, R. Rumely used Hasse's Norm Theorem.) Recently B. Poonen [7] extended the results. He proved that the theory of infinite finitely generated fields is undecidable.

As for undecidable infinite algebraic extensions of the rationals, the only known such fields are fields whose descriptions depend on non-recursive sets. For example, if we adjoin to the rationals the square roots of a non-recursive set of prime numbers, then the resulting field is certainly undecidable. (See [10].) On the other hand, J. Robinson [9] proved that the theory of the ring of all totally real algebraic integers is undecidable. We say that an algebraic number a is totally real iff a and all its conjugates are real. Then she conjectured that the field $\mathbb{Q}^{tr}$ of all totally real algebraic

numbers was undecidable. But in 1994 Fried, Haran, and Völklein [1] proved that $\mathbb{Q}^{tr}$ is decidable. So it remains open whether or not there are 'natural' undecidable infinite algebraic extensions of $\mathbb{Q}$.

In order to define the ring of algebraic integers in a given number field, J. Robinson constructed a formula which includes $\mathbb{Z}$ but excludes non-algebraic integers, which only depends on the ramification index of prime ideals of a number field which divides 2. Let F be a number field and $\psi(t)$ be such a formula. J. Robinson defined the ring of algebraic integers $\mathfrak{O}$ of F in F in the following way. Let $a_1, \ldots, a_s$ be an integral basis of $\mathfrak{O}$ ($s = [F : \mathbb{Q}]$) , and let $P_i(x)$ be the minimal polynomial of a_i over $\mathbb{Q}$ (hence over $\mathbb{Z}$) for each i. Then in F

$$t \in \mathfrak{O} \Longleftrightarrow \exists x_1, \ldots, x_s, y_1, \ldots, y_s (t = x_1 y_1 + \cdots + x_s y_s \wedge \bigwedge_i P_i(y_i) \wedge \bigwedge_i \psi(x_i))$$

holds. Note that this formula depends on F.

In this article we will show that $\psi(t)$ includes $\mathbb{Z}$ and excludes non-algebraic integers also in $K_l = \bigcup_n \mathbb{Q}(\cos(2\pi/l^n))$ with l an odd prime.

Unfortunately we cannot define the ring of algebraic integers in the same way as in number fields. Nevertheless we conjecture that $\psi(t)$ itself defines the ring of algebraic integers in K_l if $l > 5$ is a prime and $-1 \bmod 4$. If this conjecture is true, then it follows that $\mathbb{N}$ is definable in such K_l by the results of J. Robinson [9].

In section 2, we describe the construction of $\psi(t)$ in [8]. which we need in section 3. In section 3, we will prove that $\psi(t)$ includes $\mathbb{Z}$ and excludes non-algebraic integers also in $K_l = \bigcup_n \mathbb{Q}(\cos(2\pi/l^n))$ with l an odd prime. In section 4 we will prove some facts on quadratic charcters with polynomial arguments. In section 5 we will give some properties of $\psi(K_l)$.

2 Construction of $\psi(t)$

Let F be a number field (a finite algebraic extension of the rationals $\mathbb{Q}$) and let $\mathfrak{o}$ be the ring of algebraic integers of F. By $\mathfrak{p}$ we denote a valuation of F and by $F_\mathfrak{p}$ the completion of F with respect to $\mathfrak{p}$. Since non-Archemedean valuations of F are $\mathfrak{p}$-adic valuations for some prime ideal $\mathfrak{p}$ of F, we use the same letter $\mathfrak{p}$ for both the valuation and the prim ideal. Let $\mathfrak{p}$ be a prime ideal of F and $a \in F$. By $\nu_\mathfrak{p}(a)$ we denote the order of a at $\mathfrak{p}$. Given $a, b \in F^*$, we use Hilbert symbol $(a, b)_\mathfrak{p}$, which is defined to be $+1$ if $ax^2 + by^2 = 1$ is solvable in $F_\mathfrak{p}$, otherwise defined to be -1.

The following lemma is well-known:

Lemma 1 *$h \in F^*$ can be represented by the the ternary quadratic form $x^2 - ay^2 - bz^2$ iff $-ab/h \notin F_\mathfrak{p}^{*2}$ for any valuation $\mathfrak{p}$ such that $(a, b)_\mathfrak{p} = -1$.*

This follows from the property of quaternary quadratic forms and the Hasse-Minkowski theorem on quadratic forms. See [6, p. 187] and [14, p. 111].

Using this lemma, J. Robinson proved the following:

(†) *Let m be a positive integer such that $\mathfrak{p}^m \not| 2$ for all prime ideals $\mathfrak{p}$. Let $\varphi(s,u,t)$ be*

$$\exists x,y,z(1 - sut^{2m} = x^2 - sy^2 - uz^2).$$

For $t \notin \mathfrak{o}$, there are $a, b \in \mathfrak{o}$ such that

1. $F \models \neg\varphi(a,b,t)$,
2. $F \models \forall c(\varphi(a,b,c) \to \varphi(a,b,c+1))$.

Then we can use inductive form: Let $\psi(t)$ be

$$\forall s,u(\forall c(\varphi(s,u,c) \to \varphi(s,u,c+1)) \to \varphi(s,u,t)),$$

then the solution set of $\psi(t)$ in F, $\psi(F)$, includes $\mathbb{Z}$ but excludes non-algebraic integers, that is, $\mathbb{Z} \subseteq \psi(F) \subseteq \mathfrak{o}$. Since $\varphi(s,u,0)$ holds for every $s,u \in F$, the inductive form insures that every positive integer satisify ψ. Since $\varphi(s,u,t) \leftrightarrow \varphi(s,u,-t)$, every rational integer also satisfies ψ. The above statement (†) shows that non-algebraic integers fail to satisfy ψ. Note that for $t \notin \mathfrak{o}$ (and for $t \in \mathfrak{o}$), it is not so difficult to find $a, b \in F$ such that 1 holds, but difficult to find a, b such that both 1 and 2 hold.

J. Robinson proved the above statement from two lemmas. We state these two lemmas in a little bit different forms for our sake. Before stating these lemmas, we need some lemmas. The following two lemmas are special cases of a theorem proved in [4, p. 166].

Lemma 2 *There are infinitely many prime ideals in every ideal class.*

Lemma 3 *If $a \in \mathfrak{o}$ is prime to an ideal $\mathfrak{m}$, there are infinitely many prime elements $p \in \mathfrak{o}$ such that $p \equiv a \pmod{\mathfrak{m}}$.*

Lemma 4 *Let $a \in \mathfrak{o}$ and $\nu_{\mathfrak{p}}(a) = 1$. Then there is $b \in \mathfrak{o}$ with $\mathfrak{p} \not| b$ such that $(a,b)_{\mathfrak{p}} = -1$.*

Proof. It is proved in [6, pp. 161–165] that there is a unit in a local field M such that it is congruent to a square $\pmod{4\mathfrak{o}}$ but not $\pmod{4\mathfrak{p}}$, where $\mathfrak{o}$ is the ring of integers and $\mathfrak{p}$ a prime ideal of M. And if ϵ is such a unit, $(a,\epsilon)_{\mathfrak{p}} = -1$ for a prime element a. Take such a unit $\epsilon \in F_{\mathfrak{p}}$. There is a unit $\epsilon_0 \in F$ such that $\epsilon_0 \equiv \epsilon \pmod{4\mathfrak{p}}$. ϵ_0 is congruent to a square $\pmod{4\mathfrak{o}}$ but not $\pmod{4\mathfrak{p}}$. □

We state two basic lemmas due to J. Robinson [8, Lemma 8,9].

Lemma 5 *Given a prime ideal $\mathfrak{p}_1$ of F and an odd prime number l, there are relatively prime elements a and b in $\mathfrak{o}^*$ such that*

1. *$(a) = \mathfrak{p}_1 \cdots \mathfrak{p}_{2k}$, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_{2k}$ are distinct prime ideals which include every prime ideals which divides 2, and $\mathfrak{p}_j$ dose not divide l for $j = 2, \ldots, 2k$, and*

2. *b is a totally positive prime element such that $(a, b)_\mathfrak{p} = -1$ iff $\mathfrak{p}|a$.*

Proof. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_{2k-1}$ be a set of disticnt prime ideals such that it includes every prime idals dividing 2 and $\mathfrak{p}_j$ dose not divide l for $j = 2, \ldots, 2k-1$. Let $\mathfrak{K}$ be the ideal class which contains the product $\mathfrak{p}_1 \cdots \mathfrak{p}_{2k-1}$. By Lemma 2 we can choose a prime ideal $\mathfrak{p}_{2k}$ in the ideal class $\mathfrak{K}^{-1}$ with $\mathfrak{p}_{2k} \neq \mathfrak{p}_i$ for $i = 1, \ldots, 2k-1$ and with $\mathfrak{p}_{2k} \nmid (l)$.

For $i = 1, \ldots, 2k$, by Lemma 4 we can choose $b_i \in \mathfrak{o}$ prime to $\mathfrak{p}_i$ so that $(a, b_i)_{\mathfrak{p}_i} = -1$. Let m be a positive integer such that $\mathfrak{p}^m \nmid 2$ for every prime ideal $\mathfrak{p}$. Consider the simultaneous system of congruences

$$x \equiv b_i \pmod{\mathfrak{p}_i^{2m}} \quad \text{for } i = 1, \ldots, 2k.$$

By the Chinese Remainder Theorem, there is a solution $c \in \mathfrak{o}$ and so is every element which is congruent to $c \pmod{\mathfrak{p}_1^{2m} \cdots \mathfrak{p}_{2k}^{2m}}$. Since c is prime to the modulus, by Lemma 3 there are infinitely many totally positive prime elements p such that

$$p \equiv c \pmod{\mathfrak{p}_1^{2m} \cdots \mathfrak{p}_{2k}^{2m}}.$$

Let b be one of such elements. b is coprime to a.

We claim that $b_i/b \in F_{\mathfrak{p}_i}^2$ for each i ; since $b \equiv b_i \pmod{\mathfrak{p}_i^{2m}}$ and b_i is prime to $\mathfrak{p}_i$, $\nu_{\mathfrak{p}_i}(1 - b_i/b) > \nu_{\mathfrak{p}_i}(4)$, then we apply Newton's method of iteration [4, p. 42]: "Let $f(x)$ be a polynomoial with coefficients in $\mathfrak{O}_{F_{\mathfrak{p}_i}}$. If there is an element α_0 of $\mathfrak{O}_{F_{\mathfrak{p}_i}}$ such that $|f(\alpha_0)| < |f'(\alpha_0)^2|$, then $f(x)$ has a root in $\mathfrak{O}_{F_{\mathfrak{p}_i}}$." Letting $f(x) = x^2 - b_i/b$ and $\alpha_0 = 1$, we get that $b_i/b \in F_{\mathfrak{p}_i}^{*2}$. Hence $(a, b)_{\mathfrak{p}_i} = -1$ for each i. On the other hand, $(a, b)_\mathfrak{p} = +1$ for all Archimedean valuations $\mathfrak{p}$ since b is totally positive. It is easy to see that if $(a, b)_\mathfrak{p} = -1$ then $\mathfrak{p}$ is an Archimedean valuation or the prime ideal $\mathfrak{p}$ dividing $2ab$ (see [6, p. 166]). Then the only other other valuation for which $(a, b)_\mathfrak{p} = -1$ could hold would be $\mathfrak{p} = (b)$; but, by the product formula for the Hilbert symbol ([6, p. 190]), $(a, b)_\mathfrak{p} = -1$ for an even number of valuations. Therefore $(a, b)_\mathfrak{p} = -1$ iff $\mathfrak{p}|a$. □

Lemma 6 *Let $(a) = \mathfrak{p}_1 \cdots \mathfrak{p}_{2k}$ such that $\mathfrak{p}_1, \ldots, \mathfrak{p}_{2k}$ are distinct prime ideals which include every prime ideals which divides 2, and let $b \in \mathfrak{o}^*$ be coprime to a such that $(a, b)_\mathfrak{p} = -1$ iff $\mathfrak{p}|a$, and m be a positive integer such that $\mathfrak{p}^m \nmid 2$ for every prime ideal $\mathfrak{p}$. Then,*

$1 - abc^{2m} = x^2 - ay^2 - bz^2$ is solvable for x, y and z in F iff $\nu_{\mathfrak{p}_i}(c) \geq 0$ for each i.

Proof. Let $h = 1 - abc^{2m}$. Then $h \neq 0$ since $\nu_{\mathfrak{p}_1}(abc^{2m}) \neq 0$. Suppose that $\nu_{\mathfrak{p}_i}(c) \geq 0$ for each i. Since $\nu_{\mathfrak{p}_i}(h) = 0$ and $\nu_{\mathfrak{p}_i}(-ab) = 1$, $h/(-ab) \notin F_{\mathfrak{p}_i}^{*2}$ for each i. By Lemma 1 and the assumption, $h = x^2 - ay^2 - bz^2$ is solvable for x, y and z in F.

Now suppose that $\nu_{\mathfrak{p}_i}(c) < 0$ for some i. Let $\nu_{\mathfrak{p}_{i_0}}(c) < 0$. We show that $-ab/h \in F_{\mathfrak{p}_{i_0}}^2$. Since $\nu_{\mathfrak{p}_{i_0}}(1 - (-ab/h)) > \nu_{\mathfrak{p}_{i_0}}(4)$, applying again Newton's method of iteration [4, p. 42] with $x^2 - (-ab/h)$ and $\alpha_0 = 1$, we get that $-ab/h \in F_{\mathfrak{p}_{i_0}}^{*2}$. It follows that $h = x^2 - ay^2 - bz^2$ is not solvable for x, y and z in F. □

It is easy to derive the statement (†) from the above two lemmas. For $t \notin \mathfrak{O}$, take $\mathfrak{p}_1$ such that $\nu_{\mathfrak{p}_1}(t) < 0$ and $a, b \in \mathfrak{O}$ as in Lemma , then the statement (†) holds, noting $\nu_{\mathfrak{p}}(c+1) \geq 0$ if $\nu_{\mathfrak{p}}(c) \geq 0$ for every prime ideal $\mathfrak{p}$.

3 $\psi(t)$ in K_l

The following lemma on cyclotomic fields is well-known and proved in [2, pp. 256–258]. We denote by ϕ Euler's function.

Lemma 7 *Let $M = \mathbb{Q}(\zeta_m)$, where m is an positive integer and ζ_m is a primitive m-th root of unity. Then:*

1. $[M : \mathbb{Q}] = \phi(m)$.
2. *The only ramified prime ideals in M are those dividing m.*

   If $m = l^n$ with l odd prime, then there is only one prime $\mathfrak{p} = (1 - \zeta_m)$ of M lying above l, and it is totally ramified.
3. *Let p be a prime with $p \nmid m$, and let f bethe smallest positive integer such that $p^f \equiv 1 \pmod{m}$. Then in M we have $p = \mathfrak{p}_1 \cdots \mathfrak{p}_g$, where each $\mathfrak{p}_i$ has residue degree f and $fg = \phi(m)$.*

Lemma 8 *Let $F = \mathbb{Q}(\cos(2\pi/m))$ and $M = \mathbb{Q}(\zeta_m)$ be as above. Then:*

1. *$2\cos(2k\pi/m)$ with $0 \leq k \leq m$ are algebraic integers, and $2\cos(2k\pi/m)$ with $0 \leq k \leq m/2$ and $(k, m) = 1$ form a set of conjugates.*
2. *$M \supset F$, $[M : F] = 2$ (hence M is abelian extension of $\mathbb{Q}$, and $[F : \mathbb{Q}] = \phi(m)/2$).*
3. *The only ramified prime ideals in M are those dividing m.*

   If $m = l^n$ with l odd prime, then there is only one prime $\mathfrak{p} = (2 - 2\cos(2\pi/m))$ of M lying above l, and it is totally ramified, and $2\cos(2k\pi/m)$ with $0 \leq k \leq m/2$ and $(k, m) = 1$ are units in the ring of algebraic integers.

Proof. Since $2\cos(2k\pi/m) = e^{2k\pi/m} + 1/e^{2k\pi/m}$, $2\cos(2k\pi/m)$ are algebraic integers. Noting that $e^{2k\pi/m}, 1/e^{2k\pi/m}$ with $0 \leq k \leq m/2$ and $(k,m) = 1$ are primitive roots of unity, we have that $2\cos(2k\pi/m)$ with $0 \leq k \leq m/2$ and $(k,m) = 1$ form a set of conjugates. It follows that $M \supset F$,$[M : F] = 2$, and the only ramified prime ideals in M are those dividing m.

Let $m = l^n$ with l odd prime. Then,

$$(x^{l^{n-1}})^{l-1} + (x^{l^{n-1}})^{l-2} + \cdots + x^{l^{n-1}} + 1 = \prod_{\substack{0 \leq k \leq l^n/2 \\ (k,l)=1}} (x - e^{2k\pi/l^n})(x - 1/e^{2k\pi/l^n})$$

$$= \prod_{\substack{0 \leq k \leq l^n/2 \\ (k,l)=1}} (x^2 - 2\cos(2k\pi/l^n)x + 1).$$

Letting $x = 1$, we have,

$$l = \prod_{\substack{0 \leq k \leq l^n/2 \\ (k,l)=1}} (2 - 2\cos(2k\pi/l^n)).$$

Since

$$\frac{2 - 2\cos(2k_1\pi/l^n)}{2 - 2\cos(2k_2\pi/l^n)} = \frac{(1 - e^{2k_1\pi/l^n})(1 - 1/e^{2k_1\pi/l^n})}{(1 - e^{2k_2\pi/l^n})(1 - e^{2k_2\pi/l^n})},$$

$(2 - 2\cos(2k_1\pi/l^n))/(2 - 2\cos(2k_2\pi/l^n))$ are units if $k_1 \neq k_2$. Hence,

$$(l) = (2 - 2\cos(2\pi/l^n))^{\phi(l^n)}.$$

It follows that there is only one prime $\mathfrak{p} = (2 - 2\cos(2\pi/l^n))$ of M lying above l, and it is totally ramified.

Letting $x = \sqrt{-1}$, we have,

$$\pm 1 = \prod_{\substack{0 \leq k \leq l^n/2 \\ (k,l)=1}} 2\cos(2k\pi/l^n).$$

Therefore $2\cos(2k\pi/m)$ with $0 \leq k \leq m/2$ and $(k,m) = 1$ are units in the ring of algebraic integers. □

It is proved in [11] that $2\cos(2k\pi/m)$ with $0 \leq k \leq m/2$ and $(k,m) = 1$ are algebraic units iff $m \neq 1, 2, 4$ and is not of the form $4p^n$ with p prime.

From now on, let $F_n = \mathbb{Q}(\cos(2\pi/l^n))$, where l is an odd prime , and let $K_l = \bigcup_n \mathbb{Q}(\cos(2\pi/l^n))$ $(F_0 = \mathbb{Q})$. We denote by $\mathfrak{O}_n$ the ring of algebraic integers in F_n and by $\mathfrak{O}_{K_l}$ the ring of algebraic integers in K_l. Then $\mathfrak{O}_{K_l} = \bigcup_n \mathfrak{O}_n$.

From Lemma 8, we easily see that,

Lemma 9 *Let $0 < i < j$ and $\mathfrak{p}$ be a prime ideal of F_i. Then:*

1. *If $\mathfrak{p} \not| l$, then in F_j, $\mathfrak{p} = \mathfrak{P}_1 \cdots \mathfrak{P}_k$, where $\mathfrak{P}_r$ are primes in F_j and k divides $[F_j : F_i] = l^{j-i}$.*

2. *If $\mathfrak{p}|l$, then in F_j, $\mathfrak{p} = \mathfrak{P}^{l^{j-i}}$, where $\mathfrak{p} = (2-2\cos(2\pi/l^i)), \mathfrak{P} = (2-2\cos(2\pi/l^j))$.*

The next lemma is also proved in [2, p. 272].

Lemma 10 *Let $K \supset k$ number fields and $\mathfrak{P} \supset \mathfrak{p}$ be primes of K and k respectively. For $\alpha \in K_{\mathfrak{P}}^*$, let $a = N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(\alpha)$ and $b \in k_{\mathfrak{p}}$. Then, $(\alpha, b)_{\mathfrak{P}} = (a, b)_{\mathfrak{p}}$.*

The next lemma follows from Lemma 10.

Lemma 11 *Let $0 < i < j$, $\mathfrak{p}$ a prime ideal of F_i and $\mathfrak{P}$ be a prime in F_j lying over $\mathfrak{p}$. Then for $a, b \in F_i^*$, $(a, b)_{\mathfrak{p}} = 1$ iff $(a, b)_{\mathfrak{P}} = 1$.*

Proof. Since F_j/F_i is an abelian extension, the local degree at $\mathfrak{P}$ divides the degree of F_j/F_i, that is, $[(F_j)_{\mathfrak{P}} : (F_i)_{\mathfrak{p}}] | [F_j : F_i]$ (see [6, p. 32].) Let u be the local degree at $\mathfrak{P}$. Then $N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(a) = a^u$ and $(a, b)_{\mathfrak{P}} = (a^u, b)_{\mathfrak{p}} = (a, b)_{\mathfrak{p}}^u$. Since u is odd, it follows that $(a, b)_{\mathfrak{p}} = 1$ iff $(a, b)_{\mathfrak{P}} = 1$. □

We now extend J. Robinson's result [8] to K_l. Note that in each F_n, $\mathfrak{p}^2 \not| 2$ for every prime ideal in F_n.

Theorem 12 *Let $\varphi(s, u, t)$ be*

$$\exists x, y, z(1 - abt^4 = x^2 - sy^2 - uz^2)$$

and $\psi(t)$ be

$$\forall s, u(\forall c(\varphi(s, u, c) \to \varphi(s, u, c + 1)) \to \varphi(s, u, t)),$$

then the solution set of $\psi(t)$ in K_l, $\psi(K_l)$, includes $\mathbb{Z}$ but excludes non-algebraic integers, that is, $\mathbb{Z} \subseteq \psi(K_l) \subseteq \mathfrak{O}_{k_l}$.

Proof. It is clear that $\mathbb{Z} \subseteq \psi(K_l)$. Let $t \in K_l \setminus \mathfrak{O}_{K_l}$. For this t, we show that there are $a, b \in K_l$ such that

$$K_l \models \neg\varphi(a, b, t) \wedge \forall c(\varphi(a, b, c) \to \varphi(a, b, c + 1)).$$

We fix F_m such that $t \in F_m$ and $m > 1$. Then $\nu_{\mathfrak{p}_1}(t) < 0$ for some prime $\mathfrak{p}_1$ in F_m. By Lemma 2, there are relatively prime elements a and b in $\mathfrak{O}_m$ such that

1. $(a) = \mathfrak{p}_1 \cdots \mathfrak{p}_{2k}$, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_{2k}$ are distinct prime ideals in F_m which include every prime ideals in F_m which divides 2, and $\mathfrak{p}_j$ dose not divide l for $j = 2, \ldots, 2k$, and

2. b is a totally positive prime element in F_m such that $(a,b)_{\mathfrak{p}} = -1$ iff $\mathfrak{p}|a$.

By Lemma 6, $1 - abt^4 = x^2 - ay^2 - bz^2$ is not solvable for x, y and z in F_m, and for every $c \in F_m$, if $F_m \models \varphi(a,b,c)$ then $F_m \models \varphi(a,b,c+1)$.

For this a, b, it is enough to show that for every $s > m$ such that $s - m$ is even, $1 - abt^4 = x^2 - ay^2 - bz^2$ is not solvable for x, y and z in F_s, and for every $c \in F_s$, if $F_s \models \varphi(a,b,c)$ then $F_s \models \varphi(a,b,c+1)$.

Note that a, b are relatively prime also in $\mathfrak{O}_s$.

Case 1: $\mathfrak{p}_1 \nmid l$.

By Lemma 9, the decomposition of the ideal (a) in F_s is given by $(a) = \mathfrak{P}_1 \cdots \mathfrak{P}_{2r}$, where $\mathfrak{P}_1, \ldots, \mathfrak{P}_{2r}$ are mutually distinct prime ideals and include every prime ideals which devides 2. By Lemma 11, $(a,b)_{\mathfrak{P}} = -1$ iff $\mathfrak{P}|a$. We let $\mathfrak{p}_1 \subset \mathfrak{P}_1$. Since $\nu_{\mathfrak{p}_1}(t) < 0$, we have that $\nu_{\mathfrak{P}_1}(t) < 0$. By Lemma 6, we conclude that $1 - abt^4 = x^2 - ay^2 - bz^2$ is not solvable for x, y and z in F_s, and for every $c \in F_s$, if $F_s \models \varphi(a,b,c)$ then $F_s \models \varphi(a,b,c+1)$.

Case 2: $\mathfrak{p}_1|l$.

By Lemma 9, the decomposition of the ideal (a) in F_s is given by

$$(a) = \mathfrak{P}_1^{l^{s-m}} \cdots \mathfrak{P}_{2r'},$$

where $\mathfrak{P}_1, \ldots, \mathfrak{P}_{2r'}$ are mutually distinct prime ideals and include every prime ideals which devides 2, and $\mathfrak{p}_1 = (2 - 2\cos(2\pi/l^m)), \mathfrak{P}_1 = (2 - 2\cos(2\pi/l^s))$.

Let $a' = a/(2 - 2\cos(2\pi/l^s))^{l^{s-m}-1}$. Then $a' \in \mathfrak{O}_s$ and $(a') = \mathfrak{P}_1 \cdots \mathfrak{P}_{2r'}$ in F_s. Since $a = a'((2 - 2\cos(2\pi/l^s))^{(l^{s-m}-1)/2})^2$, $(a,b)_{\mathfrak{P}_i} = (a',b)_{\mathfrak{P}_i}$ for each i. Hence we have that $(a',b)_{\mathfrak{P}} = -1$ iff $\mathfrak{P}|a'$.

Suppose that $1 - abt^4 = x^2 - ay^2 - bz^2$ were solvable for x, y and z in F_s. Then

$$1 - a'b(t(2 - 2\cos(2\pi/l^s))^{(l^{s-m}-1)/4})^4 = x^2 - a'((2 - 2\cos(2\pi/l^s))^{(l^{s-m}-1)/2}y)^2 - bz^2$$

is solvable for x, y and z in F_s, noting that $(l^{s-m} - 1)/4$ is a positive integer since $l - m$ is even. But $\nu_{\mathfrak{P}_1}(t(2 - 2\cos(2\pi/l^s))^{(l^{s-m}-1)/4}) < 0$ since $\mathfrak{p}_1 = \mathfrak{P}_1^{l^{s-m}}$. We have a contradiction by Lemma 6.

Next we show that if $F_s \models \varphi(a,b,c)$ then $F_s \models \varphi(a,b,c+1)$. Suppose that $F_s \models \varphi(a,b,c)$, that is, $1 - abc^4 = x^2 - ay^2 - bz^2$ is solvable for x, y and z in F_s. Then

$$1 - a'b(c(2 - 2\cos(2\pi/l^s))^{(l^{s-n}-1)/4})^4 = x^2 - a'((2 - 2\cos(2\pi/l^s))^{(l^{s-n}-1)/2}y)^2 - bz^2$$

is solvable for x, y and z in F_s. By Lemma 6, $\nu_{\mathfrak{P}_i}(c(2 - 2\cos(2\pi/l^s))^{(l^{s-m}-1)/4}) \geq 0$ for each $\mathfrak{P}_i$. It follows that $\nu_{\mathfrak{P}_i}((c+1)(2 - 2\cos(2\pi/l^s))^{(l^{s-m}-1)/4}) \geq 0$ for each $\mathfrak{P}_i$. Therefore we have that $F_s \models \varphi(a,b,c+1)$. □

Remark 13 We can easily show the following.

1. *For every* $n \in \mathbb{Z}$, $t \in \psi(K_l)$ iff $t + n \in \psi(K_l)$,
2. *for every* $m \in \mathbb{Z}$, *if* $t \in \psi(K_l)$, *then* $mt \in \psi(K_l)$,
3. $\psi(K_l)$ *is closed under automorophism, that is, if* $a \in \psi(K_l)$, *then all conjugates of* a *are also in* K_l.

For 2., we use the equivalence $\varphi(a, b, mc) \leftrightarrow \varphi(m^2 a, m^2 b, c)$.

Remark 14 The result for K_l holds also for towers of cyclotomics similarly. Let $M_n = \mathbb{Q}(\zeta_{l^n})$, where l is an odd prime and ζ_{l^n} is a primitive l^n-th root of unity, and let $N_l = \bigcup_n \mathbb{Q}(\zeta_{l^n})$ ($M_0 = \mathbb{Q}$). We denote by $\mathfrak{O}_{N_l}$ the ring of algebraic integers in N_l. Then, $\mathbb{Z} \subseteq \psi(N_l) \subseteq \mathfrak{O}_{N_l}$.

4 quadratic characters with polynomial arguments

In this section we will prove some facts on some character sums of finite fields which we will use later. We let $\mathbb{F}_q$ be a finite field with q elements, and $q = p^f$ where p is an odd prime. We let η be the quadratic character of $\mathbb{F}_q$, that is, $\eta(0) = 0, \eta(c) = 1$ if $c \in \mathbb{F}_q^{*2}$ and $\eta(c) = -1$ otherwise.

We consider the following character sum

$$I_n(a) = \sum_{c \in \mathbb{F}_q} \eta(c^n + a),$$

where $a \in \mathbb{F}_q$. Moreover we use the following character sum

$$H_n(a) = \sum_{c \in \mathbb{F}_q} \eta(c^{n+1} + ac),$$

which is called a Jacobsthal sum. Using these character sums, we will show that if $\eta(a) = -1$, $p \equiv 3 \pmod 4$ and $p > 3$, then there are $b \in \mathbb{F}_q$ and $i \in \mathbb{F}_p$ such that $\eta(b^4 + d)\eta((b+i)^4 + d) = -1$.

Lemma 15 *Let* $p \equiv 3 \pmod 4$, $q = p^f$, *and* $a \in \mathbb{F}_q$. *Then:*

1. *If* f *is odd,* $I_4(a) = -1$.
2. *If* f *is even and* $\eta(a) = -1$, $I_4(a) = -1$.

Proof. We first note that $q \equiv 3 \pmod 4$ if f is odd and $q \equiv 1 \pmod 4$ if f is even.

For 1., it is proved in [5, pp. 231–232] that $I_2(a) = -1$ for all $a \in \mathbb{F}_q$, $I_{2n} = I_n(a) + H_n(a)$, and if the largest power of 2 dividing $q - 1$ also divides n, then $H_n(a) = 0$. Therefore we get that $H_2(a) = 0$ and $I_4(a) = -1$ for all $a \in \mathbb{F}_q$.

For 2., we use the following formula [5, p. 231].

$$I_n(a) = \eta(a) \sum_{j=1}^{d-1} \lambda^j(-a) J(\lambda^j, \eta),$$

where λ is a multicative character of $\mathbb{F}_q$ of order $d = (n, q-1)$ and $J(\lambda^j, \eta)$ is a Jacobi sum, that is,

$$J(\lambda^j, \eta) = \sum_{c_1+c_2=1} \lambda^j(c_1)\eta(c_2).$$

Letting $n = 4$, we see that λ is a multiplicative character of order 4, hence $\eta = \lambda^2$. Therefore we see by [5, p. 207] that

$$J(\lambda^2, \eta) = -\frac{1}{q} G(\eta, \chi_1)^2,$$

where $G(\eta, \chi_1)$ is a Gaussian sum. Further we know by [5, p. 199] that

$$G(\eta, \chi_1) = (-1)^{f-1} i^f q^{1/2}.$$

Therefore we get

$$I_4(a) = \eta(a) \left(\lambda(-a) J(\lambda, \eta) - \lambda^2(-a)(-1)^f + \lambda^3(-a) J(\lambda^3, \eta) \right).$$

It is easy to see that $(q-1)/4$ is even, and $\lambda(-1) = -1$ iff $(q-1)/4$ is odd, hence we see that $\lambda(-1) = 1$. Together with $\eta(-1) = (-1)^{(q-1)/2} = 1$ and $\lambda^3 = \overline{\lambda}$, we have

$$I_4(a) = \lambda^3(a) J(\lambda, \eta) + (-1)^{f+1} + \lambda(a) \overline{J(\lambda, \eta)}.$$

Here we have that $\lambda(a) = \pm i$ since $\eta(a) = -1$. Then

$$I_4(a) = -1 \pm 2 \mathrm{Im} J(\lambda, \eta).$$

We now calculate $\mathrm{Im} J(\lambda, \eta)$ of $\mathbb{F}_q$. Let $J(\lambda, \eta) = A + Bi$. A and B are rational integers since λ assumes only the values $0, \pm 1$ and $\pm i$. By [5, p. 209], we know that $|J(\lambda, \eta)| = q^{1/2}$, hence we have that $A^2 + B^2 = p^f$. It is well-known that for p such that $p \equiv 3 \pmod 4$, it is the case that $A = \pm p^{f/2}$ and $B = 0$, or vice versa. However we can show that $A = p^{f/2}$ if $f/2$ is odd, $A = -p^{f/2}$ if $f/2$ is even, and $B = 0$ by the similar way in [5, p 233], from which $I_4(a) = -1$ follows. It is proved in [5, p. 232] that

$$H_n(a) = \eta(a)\lambda(-1) \sum_{j=0}^{d-1} \lambda^{2j+1}(a) J(\lambda^{2j+1}, \eta),$$

where $d = (n, q-1)$ and λ is a multiplicative character of $\mathbb{F}_q$ of order $2d$. From this formula we get

$$H_2(1) = \lambda(-1)\left(J(\lambda,\eta) + J(\lambda^3,\eta)\right) = \lambda(-1)\left(J(\lambda,\eta) + \overline{J(\lambda,\eta)}\right) = 2\mathrm{Re}J(\lambda,\eta),$$

hence $\mathrm{Re}J(\lambda,\eta) = \frac{1}{2}H_2(1)$. We will now show that $\frac{1}{2}H_2(1) \equiv -1 \pmod 4$.

Let g be a primitive element of $\mathbb{F}_q$ and let $q = 4k+1$. Since $\eta(-1) = 1$ and $-1 = g^{2k}$, we can write

$$\begin{aligned} H_2(1) &= \sum_{i=1}^{4k} \eta(g^i)\eta((g^i)^2+1) \\ &= \sum_{i=1}^{2k} \eta(g^i)\eta((g^i)^2+1) + \sum_{i=1}^{2k} \eta(-g^i)\eta((-g^i)^2+1) \\ &= 2\sum_{i=1}^{2k} \eta(g^i)\eta((g^i)^2+1), \end{aligned}$$

so that

$$\frac{1}{2}H_2(1) = \sum_{i=1}^{2k} \eta(g^i)\eta((g^i)^2+1).$$

From $I_2(1) = -1$ we get

$$-1 = 1 + \sum_{i=1}^{4k} \eta((g^i)^2+1) = 1 + 2\sum_{i=1}^{2k} \eta((g^i)^2+1),$$

hence

$$-1 = \sum_{i=1}^{2k} \eta((g^i)^2+1).$$

By subtraction, we obtain

$$\frac{1}{2}H_2(1) + 1 = \sum_{i=1}^{2k} (\eta(g^i)-1)\eta((g^i)^2+1).$$

For $1 \le i \le 2k$, we have

$$(\eta(g^i)-1)(\eta((g^i)^2+1)-1) \equiv 0 \pmod 4 \text{ whenever } \eta((g^i)^2+1) \neq 0.$$

Thus,

$$(\eta(g^i)-1)\eta((g^i)^2+1) \equiv \eta(g^i)-1 \pmod 4 \text{ whenever } \eta((g^i)^2+1) \neq 0.$$

Now $\eta((g^i)^2+1)=0$ if and only if $i=k$ or $3k$. Consequently,

$$\begin{aligned}\frac{1}{2}H_2(1)+1 &\equiv \sum_{i=1}^{2k}(\eta(g^i)-1)-(\eta(g^k)-1)\\ &\equiv \sum_{i=1}^{2k}\eta(g^i)-(2k-1)-\eta(g^k) \pmod 4.\end{aligned}$$

Furthermore,

$$0=\sum_{i=1}^{4k}\eta(g^i)=2\sum_{i=1}^{2k}\eta(g^i)$$

and $\eta(g^k)=\lambda^2(g^k)=\lambda(-1)=-1$, so that

$$\frac{1}{2}H_2(1)+1 \equiv -2k \pmod 4.$$

Since k is even, we see that

$$\frac{1}{2}H_2(1)+1 \equiv 0 \pmod 4,$$

as claimed. □

Remark 16 Let $p \equiv 3 \pmod 4, q=p^f$, f even, and $\eta(a)=1$. Then from the proof of the above lemma, we see that $I_4(a)=-1+2\mathrm{Re}J(\lambda,\eta)$ if order of a in $\mathbb{F}_q^*$ is 0 mod 4, $I_4(a)=-1-2\mathrm{Re}J(\lambda,\eta)$ if order of a is 2 mod 4. Note that the value of $I_4(a)$ is independent of the choice of λ. Therfore $I_4(a)=-1\pm 2p^{f/2}$.

Lemma 17 *Let p be an odd prime such that $p \equiv 3 \pmod 4$, and $q=p^f$. Let $a \in \mathbb{F}_q$ and $\eta(a)=-1$. Then:*

1. *If f is even, there are $b \in \mathbb{F}_q$ and $j \in \mathbb{F}_p$ such that $\eta(b^4+a)\eta((b+j)^4+a)=-1$.*
2. *If f is odd and $p>3$, there are $b \in \mathbb{F}_q$ and $j \in \mathbb{F}_p$ such that $\eta(b^4+a)\eta((b+j)^4+a)=-1$.*
3. *If $f>1$ is odd, $p=3$, and $a \notin \mathbb{F}_3$, there are $b \in \mathbb{F}_q$ and $j \in \mathbb{F}_p$ such that $\eta(b^4+a)\eta((b+j)^4+a)=-1$.*

Proof. For 1., we first note that $x^4+a=0$ has no solutions in $\mathbb{F}_q$ since $\eta(-1)=1$ and $\eta(-a)=-1$. Suppose not. Then, for any $c\in\mathbb{F}_q$, $\eta(x^4+a)$ assumes the same value for $\{c,c+1,\dots,c+p-1\}$. Therefore, $I_4(a)$ must be 0 mod p, a contradiction.

For 2., we first note that $x^4+a=0$ has exactly two solutions in $\mathbb{F}_q$, say, $\pm e$, since $\eta(-1)=-1$ and $\eta(a)=-1$.

Suppose not. Then, for any $c\in\mathbb{F}_q$ such that $c\pm e\notin\mathbb{F}_p$, $\eta(x^4+a)$ assumes the same value for $\{c,c+1,\dots,c+p-1\}$.

If $e-(-e)=2e\notin\mathbb{F}_p$, then $\eta(x^4+a)$ assumes the same value for $\{e,e+1,\dots,e+p-1\}$ except e, and similarly for $\{-e,-e+1,\dots,-e+p-1\}$ except $-e$. Noting that $\eta(-e+j)=-\eta(e-j)$, $I_4(a)$ must be 0 mod p. Thus we get a contradiction since $I_4(a)=-1$.

If $2e\in\mathbb{F}_p$, then it follows that $\pm e,a\in\mathbb{F}_p$. Let η' be the quadratic character of $\mathbb{F}_p$. Then we see that $\eta(c)=\eta'(c)$ for all $c\in\mathbb{F}_p$ since f is odd. Therfore we have

$$\sum_{c\in\mathbb{F}_p}\eta(c)=\sum_{c\in\mathbb{F}_p}\eta'(c)=-1$$

So it is not the case that $\eta(x^4+a)$ assumes the same value for $\{0,1,\dots,p-1\}$ except $\pm e$ since $p\geq 7$. Hence there are $b\in\mathbb{F}_q$ and $i\in\mathbb{F}_p$ such that $\eta(b^4+a)\eta((b+i)^4+a)=-1$.

For 3., noting that $\pm e\notin\mathbb{F}_3$, we can prove the assertion. □

There are no elements $b,j\in\mathbb{F}_3$ such that $\eta(b^4+a)\eta((b+j)^4+a)=-1$, for 2 is the only element such that $\eta(2)=-1$ and $\eta(1^4+2)=\eta(2^4+2)=0$. For $\mathbb{F}_{3^f}$ with f odd and $a=2$, we cannot say whether or not there are $b\in\mathbb{F}_q$ and $j\in\mathbb{F}_p$ such that $\eta(b^4+a)\eta((b+j)^4+a)=-1$ in general.

On the other hand, we cannot establish an explicit formula for $q=p^f$ with $p\equiv 1\pmod 4$. For example, in $\mathbb{F}_5$, $\eta(2)=-1$ and $I_4(2)=-5$, $\eta(3)=-1$ and $I_4(3)=3$.

However we are interested in residue fields of $F_n=\mathbb{Q}(\cos(2\pi/l^n)$ with $l>5$. Let $\mathfrak{p}$ be a prime of F_n lying above a rational prime p. Then the residue degree $f_\mathfrak{p}$ of $\mathfrak{p}$ is determined as follows: $f_\mathfrak{p}=1$ for $\mathfrak{p}$ lying above l, and for $\mathfrak{p}$ lying above $p\neq l$, let f be the smallest positive integer such that $p^f\equiv 1\pmod{l^n}$, then $f_\mathfrak{p}$ is either f or $f/2$.

From now on, we let l be a prime greater than 5 and let p be an odd prime other tha l. We denote by $\mathfrak{p}_n$ one of primes of F_n such that $p\subset\mathfrak{p}_1\subset\mathfrak{p}_2\subset\mathfrak{p}_3\subset\cdots$, and denote by f_n the residue degree of F_n at $\mathfrak{p}_n$, that is, $\mathbb{F}_{p^{f_n}}=\mathfrak{O}_n/\mathfrak{p}_n$, where $\mathfrak{O}_n$ denotes the ring of algebraic integers of F_n. We denote $\mathbb{F}_{p^{f_n}}$ by $\bar{F}_n$. Obviously, $\mathbb{F}_p\subset\bar{F}_1\subset\bar{F}_2\subset\cdots$.

Since f_1 is either the order of p mod l or its half, hence $(f_1,l)=1$. Let $p^{f_1}=1+kl$. We easily see that if $(k,l)=1$, then $f_n=f_1l^{n-1}$ for all n, and if $k=l^bg$ with $\gcd(g,l)=1$ and $b>1$, then $f_1=f_2=\cdots=f_{b+1}$ and $f_{b+h}=f_1l^{h-1}$ if $h>1$. In either case, there is n_0 such that $f_{m+1}=f_ml$ for all $m\geq n_0$.

We again easily see that if $\eta(c)=1$ in $\bar{F}_n$ with $n\geq 1$, then $\eta(c)=1$ in $\bar{F}_m$ for all $m>n$, and similarly for $\eta(c)=-1$ in $\bar{F}_n$. So we use the same symbol η for character

sums of all $\bar{F}_n$ with $n \geq 1$. We denote by η' the quadratic character of $\mathbb{F}_p$. Note that if $l \equiv -1 \pmod 4$, then $\eta'(c) = \eta(c)$ for all $c \in \mathbb{F}_p$ since $[F_1 : \mathbb{Q}] = (l-1)/2$ is odd, and in case of $l \equiv 1 \pmod 4$, $\eta'(c) = 1$ for all $c \in \mathbb{F}_p$ if f_1 is even and $\eta'(c) = \eta(c)$ for all $c \in \mathbb{F}_p$ since $[F_1 : \mathbb{Q}] = (l-1)/2]$ is even.

We first deal with the case of $\mathbb{F}_{3^f}$ with f odd and $a = 2$. Note that 2 is the only element of $\mathbb{F}_3$ with $\eta(a) = -1$.

Lemma 18 *Let $p = 3$ and $l \equiv -1 \pmod 4$. Then there is N such that there are $b \in \bar{F}_n$ and $j \in \mathbb{F}_3$ such that $\eta(b^4+2)\eta((b+j)^4+2) = -1$ for all $n \geq N$.*

Proof. We will show that if $f \geq 3$ is odd, then there are $b \in \mathbb{F}_{3^f}$ and $j \in \mathbb{F}_3$ such that $\eta(b^4+2)\eta((b+j)^4+2) = -1$. Suppose not. Since $I_4(2) = -1$, $\eta(2) = -1$, and $\eta(1^4+2) = \eta(2^4+2) = 0$, we have $\sum_{c \in \mathbb{F}_{3^f} \setminus \mathbb{F}_3} \eta(c^4+2) = 0$. Let $q = 3^f$. Since the solution of $x^4+2 = 0$ in $\mathbb{F}_q$ are $\{1, 2\}$, the number of the set $A = \{c \in \mathbb{F}_q \setminus \mathbb{F}_3 : \eta(c^4+2) = 1\}$ is $(q-3)/2$.

Now we consider the following system of equations.

$$\begin{aligned} y^2 - x^4 + 1 &= 0 \\ z^2 - (x+1)^4 + 1 &= 0 \\ w^2 - (x+2)^4 + 1 &= 0 \end{aligned}$$

We consider the number of common solutions of these equations in $\mathbb{F}_q^4$. By assumption we have $\eta(c^4+2) = \eta((c+1)^4+2) = \eta((c+2)^4+2) = 1$ or $\eta(c^4+2) = \eta((c+1)^4+2) = \eta((c+2)^4+2) = -1$ for any $c \in \mathbb{F}_q \setminus \mathbb{F}_3$. Therefore the number of common solutions is $(q-1)/2 \times (q-1)^3 = (q-1)^4/2$.

On the other hand, the equation

$$(y^2 - x^4 + 1)(z^2 - (x+1)^4 + 1)(w^2 - (x+2)^4 +) = 0$$

has at most $12q^3$ solutions in $\mathbb{F}_q^3$ by [5, p. 275]. Hence we get $(q-1)^4 < 12q^3$, a contradiction since $q \geq 3^3 = 27$.

As for $\bar{F}_n = \mathbb{F}_{3^{f_n}}$, every f_n is odd since $l \equiv -1 \pmod 4$, and obviously there is N such that $3 \leq f_N \leq f_{N+1} \leq f_{N+2} \leq \cdots$. □

Lemma 19 *We let $p \equiv 1 \pmod 4$. For any $n \geq 1$ and for any $a \in \bar{F}_n$ with $\eta(a) = -1$, there is $N > n$ such that there are $b \in \bar{F}_N$ and $j \in \mathbb{F}_p$ such that $\eta(b^4+a)\eta((b+j)^4+a) = -1$.*

Proof. We first note that $\eta(-1) = 1$ in all $\bar{F}_m$ since every power of p is 1 mod 4, hence $x^4 + a = 0$ has no solutions in all $\bar{F}_m$.

Fix n and $a \in \bar{F}_n$ with $\eta(a) = -1$. Take an integer n' such that $n' > \max(n, n_0)$. If p dose not divide $\sum_{c \in \bar{F}_{n'}} \eta(c^4 + a)$, we are done. Suppose that p divides $\sum_{c \in \bar{F}_{n'}} \eta(c^4 + a)$. Here $\bar{F}_{n'} = \mathbb{F}_{p^{f_{n'}}}$. Let $q = p^{f_{n'}}$. We again use the formula

$$I_n(a) = \eta(a) \sum_{j=1}^{d-1} \lambda^j(-a) J(\lambda^j, \eta),$$

We have that

$$J(\lambda^2, \eta) = -\frac{1}{q} G(\eta, \chi_1)^2,$$

as before. But this time we have by [5, p. 199] that

$$G(\eta, \chi_1) = (-1)^{f-1} q^{1/2}.$$

Therefore we get

$$I_4(a) = \eta(a) \left(\lambda(-a) J(\lambda, \eta) - \lambda^2(-a) + \lambda^3(-a) J(\lambda^3, \eta) \right).$$

Since $\eta = \lambda^2$ and $\eta(-1) = 1$, we have

$$I_4(a) = \lambda^3(-a) J(\lambda, \eta) - 1 + \lambda(-a) \overline{J(\lambda, \eta)}.$$

Here we have that $\lambda(-a) = \pm i$ since $\eta(-a) = -1$. Then

$$I_4(a) = \begin{cases} -1 + 2\mathrm{Im} J(\lambda, \eta) & \text{if } \lambda(-a) = i \\ -1 - 2\mathrm{Im} J(\lambda, \eta) & \text{if } \lambda(-a) = -i \end{cases}$$

We can show that $\mathrm{Re} J(\lambda, \eta) = \frac{1}{2} \lambda(-1) H_2(1)$ in the same way as before. We also can show that $\mathrm{Im} J(\lambda, \eta) = \frac{1}{2} \lambda(-1) H_2(d)$ for any $b \in \mathbb{F}_q$ with $\eta(d) = -1$ similarly. Note that $\lambda(-1) = \pm 1$ since $\eta(-1) = 1$. We see that $\lambda(-1) = 1$ if $q \equiv 1 \pmod 8$, and $\lambda(-1) = -1$ if $q \equiv 5 \pmod 8$

At the same time We can show that $\frac{1}{2} H_2(1) \equiv -1 \pmod 4$ in the similar way as before. Further we can show that $\frac{1}{2} H_2(d) \equiv -2k \pmod 4$ with $k = (q-1)/4$ similarly.

We will show that in $\bar{F}_{n'+1} = \mathbb{F}_{q^l}$, there are $b \in \mathbb{F}_{q^l}$ and $j \in \mathbb{F}_p$ such that $\eta(b^4 + a)\eta((b+j)^4 + a) = -1$. It is enough to show that $\sum_{c \in \mathbb{F}_{q^l}} I_4(a)$ is not divisible by p. It is proved in [5, p. 210] that

$$J(\lambda'_1, \ldots, \lambda'_k) = (-1)^{(s-1)(k-1)} J(\lambda_1, \ldots, \lambda_k)^s,$$

where $\lambda_1, \ldots, \lambda_k$ are multiplicative characters of $\mathbb{F}_q$, not all of which are trivial, and which are lifted to characters $\lambda'_1, \ldots, \lambda'_k$, respectively, of $\mathbb{F}_{q^l}$.

We say that λ_j is lifted to λ'_j if $\lambda'(c) = \lambda(\mathrm{N}_{\mathbb{F}_{q^l}/\mathbb{F}_q}(c))$ for all $c \in \mathbb{F}_{q^l}$. The quadratic character of $\mathbb{F}_q$ is lifted to the quadratic character of $\mathbb{F}_{q^l}$, and characters of order 4 of $\mathbb{F}_q$ are lifted to characters of order 4 of $\mathbb{F}_{q^l}$, since $\mathrm{N}_{\mathbb{F}_{q^l}/\mathbb{F}_q}(c) = cc^q \cdots c^{q^{l-1}} = c^{(q^l-1)/(q-1)}$ and $(q^l-1)/(q-1)$ is odd. Note that for $c \in \mathbb{F}_q$, $\eta'(c) = \eta(c)$ as stated before. Now we consider characters of order 4. Note that there are two characters of order 4 in $\mathbb{F}_q$ if $q \equiv 1 \pmod 4$, and there are none if $q \equiv -1 \pmod 4$. Let λ be a quadratic character of $\mathbb{F}_q$ and λ be lifted to λ' of $\mathbb{F}_{q^l}$. Obviously, for $c \in \mathbb{F}_q$ with $\lambda(c) = \pm 1$, we have that $\lambda'(c) = \pm 1$, respectively. Since $(q^l-1)/(q-1) \equiv l \pmod 4$, we have that, for $c \in \mathbb{F}_q$ with $\lambda(c) = \pm i$, $\lambda'(c) = \pm i$ if $l \equiv 1 \pmod 4$ respectively, and $\lambda'(c) = \mp i$ if $l \equiv -1 \pmod 4$ respectively.

Consequently, we have that $J(\lambda', \eta) = J(\lambda, \eta)^l$, $\lambda'(-a) = \lambda(-a)$ if $l \equiv 1 \pmod 4$, and $\lambda'(-a) = \overline{\lambda(-a)}$ if $l \equiv -1 \pmod 4$.

On the other hand, also in $\mathbb{F}_{q^l}$, we have

$$I_4(a) = \begin{cases} -1 + 2\mathrm{Im}J(\lambda', \eta) & \text{if } \lambda'(-a) = i \\ -1 - 2\mathrm{Im}J(\lambda', \eta) & \text{if } \lambda'(-a) = -i \end{cases}$$

similarly.

We first let $l \equiv -1 \pmod 4$. Let $I'_4(a)$ denote the character sum in $\mathbb{F}_{q^l}$ and let $J(\lambda, \eta) = A + Bi, J(\lambda', \eta) = A' + B'i$. If $\lambda(-a) = \pm i$, then $I_4(a) = -1 \pm 2B$ and $I'_4(a) = -1 \mp 2B'$, respectively. Since $J(\lambda', \eta) = J(\lambda, \eta)^l$, we have $A' + B'i = (A + Bi)^l$. Hence we get

$$B' = \binom{l}{1} A^{l-1}B - \binom{l}{3} A^{l-3}B^3 + \cdots + (-1)^{(j-1)/2} \binom{l}{j} A^{l-j}B^j + \cdots - B^l.$$

Let $\lambda(-a) = i$. By the assumption that $I_4(a) \equiv 0 \pmod p$, we have $B \equiv 1/2 \pmod p$. On the other hand, by $|J(\lambda, \eta)| = q^{1/2}$, we have $A^2 \equiv -1/4 \pmod p$. Hence we get $B' \equiv -1 \pmod p$ and $I'_4(a) = -1 - 2B' \equiv 1 \pmod p$. In case of $\lambda(-a) = i$, we have that $B' \equiv 0 \pmod p$ and $I'_4(a) = -1 - 2B' \equiv -1 \pmod p$. Thus we are done.

Secondly, we let $l \equiv 1 \pmod 4$. Then, if $\lambda(-a) = \pm i$, $I_4(a) = -1 \pm 2B$ and $I'_4(a) = -1 \pm 2B'$, respectively. Similarly, we have that $B' \equiv -1 \pmod p$ and $I'_4(a) = -1 + 2B' \equiv -3 \pmod p$ if $\lambda(-a) = i$, and $B' \equiv 0 \pmod p$ and $I'_4(a) = -1 - 2B' \equiv -1 \pmod p$ if $\lambda(-a) = i$. Thus we are done since $p \equiv 1 \pmod 4$. □

In $\mathbb{F}_5$, there is $a \in \mathbb{F}_5$ with $\eta'(a) = -1$ such that there are no b and no $j \in \mathbb{F}_5$ such that $\eta(b^4 + a)\eta((b+j)^4 + a) = -1$: take $a = 2$, then $\eta'(2) = \eta'(1+2) = \eta'(2^4+2) = \cdots = \eta'(4^4+2) = -1$. In case of $l \equiv 1 \pmod 4$ and $\eta(c) = 1$ for all $c \in \mathbb{F}_5$ (for example, let $l = 13$), we dont know that whether or not there is $N \geq 1$ in which there are $b \in \bar{F}_N$ and $j \in \mathbb{F}_5$ such that $\eta(b^4 + 2)\eta((b+j)^4 + 2) = -1$. However for primes greater than 5, we have the following:

Lemma 20 *Let p be a prime greater than 5, then there are $b, j \in \mathbb{F}_p$ such that $\eta(b^4+a)\eta((b+j)^4+a) = -1$ for any $a \in \mathbb{F}_p$.*

Proof. From the formula

$$I_n(a) = \eta(a)\sum_{j=1}^{d-1}\lambda^j(-a)J(\lambda^j,\eta),$$

we get $|I_4(a)| \leq (d-1)p^{1/2}$, where $d = (4, p-1)$. Hence $|I_4(a)| \leq 3\sqrt{p}$ if $p \equiv 1 \pmod 4$, and $|I_4(a)| \leq \sqrt{p}$ if $p \equiv -1 \pmod 4$. Therefore $|I_4(a)| < p-2$, and the assertion follows since x^4+a has possively two solutions in case of $p \equiv -1 \pmod 4$ and $\eta'(a) = -1$. □

5 Some properties of $\psi(K_l)$

In this section we let l is a prime greater than 5 and -1 mod 4, and we keep the notation of section 2. Note that under the assumption of l, $[F_n : \mathbb{Q}]$ is odd for all n.

We will give some properties of $\psi(t)$. We recall that $\psi(t)$ is a formula

$$\forall s, u(\forall c(\varphi(s,u,c) \to \varphi(s,u,c+1)) \to \varphi(s,u,t)),$$

and $\varphi(s,u,t)$ is a formula

$$\exists x, y, z(1 - abt^4 = x^2 - sy^2 - uz^2).$$

For $a, b \in F_n$, we let $S_n = \{\mathfrak{p}\text{prime spots on } F_n : (a,b)_\mathfrak{p} = -1\}$, and let $H_n = \{(a,b) \in F_n \times F_n : \text{all spots in } S_n \text{ divide } 2\}$.

Furthermore we recall that there are $a, b \in K_l$ such that

$$\begin{aligned} K_l &\models \forall c(\varphi(a,b,c) \to \varphi(a,b,c+1)) \to \varphi(a,b,t)) \text{ and} \\ K_l &\models \exists x, y, z(1 - ab\alpha^4 = x^2 - sy^2 - uz^2) \text{ for any } \alpha \in \mathfrak{O}_{k_l}, \end{aligned}$$

and in F_n such that $a, b \in F_n$, $\nu_\mathfrak{p}(-ab) \geq 1$ for all $\mathfrak{p} \in S_n$ and $\nu_\mathfrak{p}(-ab)$ is odd if $\mathfrak{p}|2$ by the proof of Theorem 12.

Generally we can prove the following proposition. From now on the ring of integers of $(F_n)_\mathfrak{p}$ is denoted by $(\mathfrak{o}_n)_\mathfrak{p}$, its maximal ideal is also denoted by $\mathfrak{p}$, its residue field $(\mathfrak{o}_n)_\mathfrak{p}/\mathfrak{p}$ by $\overline{(F_n)_\mathfrak{p}}$, and the group of units in $(\mathfrak{o}_n)_\mathfrak{p}$ by $(U_n)_\mathfrak{p}$. For $\alpha \in \mathbb{F}_n$, we denote by $\bar{\alpha}$ its residue class in $\overline{(F_n)_\mathfrak{p}}$. Further we let $\mathfrak{p}$ lie above a rational prime p.

Proposition 21 *Let $a, b \in K_l^*$ and suppose that*

$$K_l \models \forall c(\varphi(a,b,c) \to \varphi(a,b,c+1))$$

and in F_n such that $a, b \in F_n$, $\nu_\mathfrak{p}(-ab) \geq 1$ for all $\mathfrak{p} \in S_n$ and $\nu_\mathfrak{p}(-ab)$ is odd if $\mathfrak{p}|2$.

Then we have $K_l \models \varphi(a,b,\alpha)$ for all $\alpha \in \mathfrak{O}_{K_l}$.

Proof. Suppose that $K_l \models \neg\varphi(a,b,\alpha)$ for some $\alpha \in \mathfrak{O}_{K_l}$. Fix such α. Since $K_l \models \varphi(a,b,j)$ for all $j \in \mathbb{Z}$, we have $\alpha \notin \mathbb{Z}$. We easily see that $1-ab\alpha^4 \neq 0$. Take n_0 be such that $\alpha, a, b \in F_{n_0}$, then we have $n_0 > 0$ and

$$F_{n_0} \models \neg\varphi(a,b,\alpha).$$

By Lemma 1, we have

$$(1-ab\alpha^4)/(-ab) = \alpha^4 - 1/ab \in (F_{n_0})^{*2}_{\mathfrak{p}_0}$$

for some $\mathfrak{p}_0$ such that $(a,b)_{\mathfrak{p}_0} = -1$. Fix such $\mathfrak{p}_0$.

We claim that $\mathfrak{p}_0$ is not Archimedian. Suppose that $\mathfrak{p}_0$ is Archimedian. Then there is $m \in \mathbb{N}$ such that $m^4 - 1/ab \in (F_{n_0})^{*2}_{\mathfrak{p}_0}$. We can take $n_1 > n_0$ such that $F_{n_1} \models \varphi(a,b,m)$ since $K_l \models \varphi(a,b,m)$. Let $\mathfrak{p}'_0$ be a valuation of F_{n_1} lying above $\mathfrak{p}_0$. Then we have $m^4 - 1/ab \in (F_{n_1})^{*2}_{\mathfrak{p}'_0}$. Since $(F_{n_0})_{\mathfrak{p}_0} = (F_{n_1})_{\mathfrak{p}'_0} \simeq \mathbb{R}$, we have $(a,b)_{\mathfrak{p}'_0} = -1$. Hence by Lemma 1, we have $F_{n_1} \models \neg\varphi(a,b,m)$, a contradiction. Therfore $\mathfrak{p}_0$ is not Archimedian.

We have $S_{n_0} \neq \emptyset$, and for $n > n_0$, S_n consists of primes of F_n which lie above each prime in S_{n_0}, by Lemma 10 and by the above argument for Archimedian ones. We see that every prime in S_{n_0} is not Archimedian similarly.

<u>case 1:</u>$\mathfrak{p}_0 \nmid 2$.

We claim that if $n \geq n_0$, $\nu_{\mathfrak{p}}(-ab) = 0$ for $\mathfrak{p} \in S_n$ lying above $\mathfrak{p}_0$. Fix such $\mathfrak{p}$ and n. We note that $-ab \notin (F_n)^{*2}_{\mathfrak{p}}$ for all $n \geq n_0$ and for all $\mathfrak{p} \in S_n$, since $(a,b)_{\mathfrak{p}} = (a,-ab)_{\mathfrak{p}} = -1$. We can take $n' > n$ such that $F_{n'} \models \varphi(a,b,1)$ since $K_l \models \varphi(a,b,1)$. Let $\mathfrak{p}'$ be a prime of $F_{n'}$ lying above $\mathfrak{p}$. Then we have

$$(1-ab)/(-ab) = 1 - 1/ab \notin (F_{n'})^{*2}_{\mathfrak{p}'}.$$

It is known that $1+\mathfrak{p} = (1+\mathfrak{p})^2$ for $\mathfrak{p} \nmid 2$ ([6, pp. 163]). Hence $\nu_{\mathfrak{p}'}(-1/ab) \leq 0$, so $\nu_{\mathfrak{p}'}(-ab) \geq 0$. On the other hand, we have

$$(1-ab\alpha^4)/(-ab) = \alpha^4 - 1/ab \in (F_{n'})\mathfrak{p}'^{*2}$$

since $(F_{n_0})_{\mathfrak{p}_0} \subseteq (F_{n'})_{\mathfrak{p}'}$.

If $\nu_{\mathfrak{p}'}(-ab) > 0$, then $1 - ab\alpha^4 \in (F_{n'})^{*2}_{\mathfrak{p}'}$ since $\alpha \in \mathfrak{O}_{n'}$, hence $-ab \in F^{*2}_{\mathfrak{p}'}$, a contradiction. Therefore we have $\nu_{\mathfrak{p}'}(-ab) = 0$, and $\nu_{\mathfrak{p}}(-ab) = 0$, a contradiction.

<u>Case 2:</u>$\mathfrak{p}_0 | 2$.

We first note that $\nu_{\mathfrak{p}_0}(2) = 1$ since $\mathfrak{p}_0$ is unramified. Similarly as before, we have

$$-1/ab \notin (F_{n_0})^{*2}_{\mathfrak{p}_0} \tag{1}$$

$$(1-ab)/(-ab) = 1 - 1/ab \notin (F_{n_0})^{*2}_{\mathfrak{p}_0} \tag{2}$$

$$(1-ab\alpha^4)/(-ab) = \alpha^4 - 1/ab \in (F_{n_0})^{*2}_{\mathfrak{p}_0} \tag{3}$$

It is known that $(1+\mathfrak{p}^r)^2 = 1+2\mathfrak{p}^r$ if $\mathfrak{p}^r \subseteq 2\mathfrak{p}$ ([6, pp. 163]). So we have $1+\mathfrak{p}_{\mathfrak{p}_0}^3 = (1+\mathfrak{p}_{\mathfrak{p}_0}^2)^2$. Hence we have $\nu_{\mathfrak{p}_0}(-1/ab) < 3$ by (2) and $\nu_{\mathfrak{p}_0}(-ab) < 3$ by (3). It follows that $-3 < \nu_{\mathfrak{p}_0}(-ab) < 3$. Further we see that $0 \leq \nu_{\mathfrak{p}_0}(\alpha) < 2$ by (3). If $\nu_{\mathfrak{p}_0}(-1/ab) = -1$, then we have $\nu_{\mathfrak{p}_0}(\alpha^4 - 1/ab) = -1$, a contradiction since $\alpha^4 - 1/ab \in (F_{n_0})_{\mathfrak{p}_0}^{*2}$. Therefore we have $\nu_{\mathfrak{p}_0}(-1/ab) \neq -1$.

We will show that $\nu_{\mathfrak{p}_0}(\alpha) = 0$. Suppose that $\nu_{\mathfrak{p}_0}(\alpha) = 1$. In case $\nu_{\mathfrak{p}_0}(-1/ab) < 0$, we have $1 - ab\alpha^4 \in (F_{n_0})_{\mathfrak{p}_0}^{*2}$, hence $-ab \in (F_{n_0})_{\mathfrak{p}_0}^{*2}$ by (3), a contradiction. In case $\nu_{\mathfrak{p}_0}(-1/ab) > 0$, let $A = 1 - 1/ab, B = \alpha^4 - 1/ab$. Then we have $A \equiv B \pmod{\mathfrak{p}_0^3}$. Noting $A \neq 0$ and $\nu_{\mathfrak{p}_0}(A) = 0$, we have $B/A \equiv 1 \pmod{\mathfrak{p}_0^3}$, hence $B/A \in (F_{n_0})_{\mathfrak{p}_0}^{*2}$ and so $A \in (F_{n_0})_{\mathfrak{p}_0}^{*2}$, a contradiction. In case $\nu_{\mathfrak{p}_0}(-1/ab) = 0$, letting $A = -1/ab$ we would have $A \in (F_{n_0})_{\mathfrak{p}_0}^{*2}$, a contradiction. Thus we see that $\nu_{\mathfrak{p}_0}(\alpha) = 0$.

Let C be the group of $(N\mathfrak{p}-1)^{th}$ roots of unity in $(F_{n_0})_{\mathfrak{p}_0}$. Every elements of C are squares in $(F_{n_0})_{\mathfrak{p}_0}$. Let $C^* = C \cup \{0\}$. Let $\delta \in (U_{n_0})_{\mathfrak{p}_0}$. We can wright $\delta = c_0 + c_1 2 + c_2 2^2 + \cdots$, for some $c_i \in C'$ with $c_0 \neq 0$. We easily see that $\delta \in (F_{n_0})_{\mathfrak{p}_0}^2$ iff $c_1 = 0$ and $c_2/c_0 \equiv c(c+1) \pmod{\mathfrak{p}_0}$ for some $c \in C'$. If $\nu_{\mathfrak{p}_0}(-1/ab) = 1$, then we have $\alpha^4 - 1/ab \notin (F_{n_0})_{\mathfrak{p}_0}^{*2}$ since $\alpha^4 \equiv c_0^4 \pmod{\mathfrak{p}_0^3}$ for some $c_0 \neq 0$ in C. Hence we see that $\nu_{\mathfrak{p}_0}(-1/ab) \neq 1$ by (3). Accordingly $\nu_{\mathfrak{p}_0}(-1/ab) = 0$ or ± 2,hence $\nu_{\mathfrak{p}_0}(-ab) = 0$ or ± 2, a contradiction. □

Furthermore we can prove the following.

Proposition 22 *Let $a, b \in K_l^*$ and suppose that*

$$K_l \models \forall c(\varphi(a,b,c) \to \varphi(a,b,c+1))$$

and in F_n such that $a, b \in F_n$, $\nu_{\mathfrak{p}}(-ab) = 0$ and $\mathfrak{p} \not| 2$ for all $\mathfrak{p} \in S_n$.

Then we have $K_l \models \varphi(a,b,\alpha)$ for all $\alpha \in \mathfrak{O}_{K_l}$.

Proof. Suppse that $K_l \models \neg\varphi(a,b,\alpha)$ for some $\alpha \in \mathfrak{O}_{K_l}$. Fix such *alpha*. Then we have $\alpha^4 - 1/ab \notin (F_{n_0})_{\mathfrak{p}_0}^{*2}$ for some n_0 and $\mathfrak{p}_0$ a spot $\mathfrak{p}_0$ of F_{n_0}. We see that $\mathfrak{p}_0$ is a prime of F_{n_0} as before.

It is known that for $\alpha \in (U_n)_{\mathfrak{p}}$, $\alpha \in (F_n)_{\mathfrak{p}}^{*2}$ iff $\eta(\bar{\alpha}) = 1$ in $\overline{(F_n)_{\mathfrak{p}}}$ in case $\mathfrak{p} \not| 2$. Hence we see that $\eta(\overline{-1/ab}) = -1$ in $(F_n)_{\mathfrak{p}}^{*2}$ with $n \geq n_0$ and $\mathfrak{p}|\mathfrak{p}_0$. Let $d = -1/ab$. By Lemma 17, 18, 19, there are $n_1 \geq n_0$, $\mathfrak{P}_1$ a prime of F_{n_1} with $\mathfrak{P}_1|\mathfrak{p}_0$, $\bar{b} \in \overline{(F_{n_1})_{\mathfrak{P}_1}}$, and $j_0 \in \{1, \ldots, p-1\}$ such that $\eta(\bar{b}^4 + \bar{d})\eta((\bar{b}+\bar{j}_0)^4 + \bar{d}) = -1$ in $\overline{(F_{n_1})_{\mathfrak{P}_1}}$. We may assume that $\eta(\bar{b}^4 + \bar{d}) = -1$ and $\eta((\bar{b}+\bar{j}_0)^4 + \bar{d}) = 1$ without of loss of generality.

We can take $\beta \in \mathfrak{O}_{n_1}$ such that $\bar{\beta} = \bar{b}$ since $\mathfrak{O}_{n_1}/\mathfrak{P}_1 \simeq \mathfrak{o}_{n_1}/\mathfrak{P}_1$. Let $S_{n_1} = \{\mathfrak{P}_1, \ldots, \mathfrak{P}_k\}$. By the Chinese Remainder Theorem, there are $\gamma \in \mathfrak{O}_n$ such that

$$\begin{aligned} \gamma &\equiv \beta \pmod{\mathfrak{P}_1} \\ \gamma &\equiv 1 \pmod{\mathfrak{P}_i} \text{ if } \mathfrak{P}_i \not| 2, \\ \gamma &\equiv 3 \pmod{\mathfrak{P}_j^3} \text{ if } \mathfrak{P}_j | 2. \end{aligned}$$

For $\mathfrak{P}_i \not| 2$, we claim that $\gamma^4 - 1/ab \notin (F_{n_1})^{*2}_{\mathfrak{P}_i}$. Since $\bar{\gamma} = \bar{\beta}$ in $\overline{(F_{n_1})_{\mathfrak{P}_1}}$, we have that $\gamma^4 - 1/ab \notin (F_{n_1})^{*2}_{\mathfrak{P}_1}$. Let $\mathfrak{P}_i \not| 2$ with $i \neq 1$. Take $n' > n_1$ so that $F_{n'} \models \varphi(a, b, 1)$. Let $\mathfrak{P}'$ be a prime of $F_{n'}$ lying above $\mathfrak{P}_i$. Then we have

$$(1 - ab)/(-ab) = 1 - 1/ab \notin F^{*2}_{\mathfrak{P}'},$$

hence $1 - 1/ab \notin F^{*2}_{\mathfrak{P}_i}$. Since $\bar{\gamma} = \bar{1}$ in $\overline{(F_{n_1})_{\mathfrak{P}_i}}$, we are done.

For $\mathfrak{P}_j | 2$, we see that $\gamma \notin (F_{n_1})^{*2}_{\mathfrak{P}_j}$ since $\nu_{\mathfrak{P}_j}(2) = 1$ and $3 + \mathfrak{P}_j^3 = 1 + 2 + \mathfrak{P}_j^3 \notin (U_{n_1})^2_{\mathfrak{P}_j}$. Consequently we have that $F_{n_1} \models \varphi(a, b, \gamma)$, hence $K_l \models \varphi(a, b, \gamma)$.

Now since $\eta((\bar{b} + j_0)^4 + \bar{d}) = 1$ in $\overline{(F_{n_1})_{\mathfrak{P}_1}}$, we see that $(\gamma + j_0)^4 - 1/ab \in (F_{n_1})^{*2}_{\mathfrak{P}_j}$, hence we have that $F_{n_1} \models \neg\varphi(a, b, \gamma + j_0)$. We claim that $K_l \models \neg\varphi(a, b, \gamma + j_0)$. It is enough to show that $F_{n'} \models \neg\varphi(a, b, \gamma + j_0)$ for all $n' > n_1$. Take $n' > n_1$ and a prime $\mathfrak{P}'$ of $F_{n'}$ lying above $\mathfrak{P}_1$. Then since $\eta((\bar{\gamma} + j_0)^4 + \bar{d}) = 1$ also in $\overline{(F_{n'})_{\mathfrak{P}'}}$, we know that $(\gamma + j)^4 - 1/ab \in (F_{n'})^{*2}_{\mathfrak{P}'}$, hence we have that $F_{n'} \models \neg\varphi(a, b, \gamma + j_0)$.

Therefore we get $K_l \models \varphi(a, b, \gamma) \wedge \neg\varphi(a, b, \gamma + j_0)$, a contradiction, since $K_l \models \forall c(\varphi(a, b, c) \to \varphi(a, b, c + 1))$. □

References

[1] Fried, M.D., Haran, D. and Völklein, H., *Real Hilbertianity amd the Field of Toatally Real Numbers*, Contemp. Mathematics, 174 (1994), pp. 1–34.

[2] Iyanaga, S.(Editor), *The Theory of Numbers*, North-Holland Publishing Company, 1975.

[3] Kronecker, L., *Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten*, Reine. Angew. Math., 53 (1857), pp. 173–175.

[4] Lang, S., *Algebraic Number Theory*, 2nd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 1994.

[5] Lidl, R. and Niederreiter, H., *Finite fields*, Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, 1997.

[6] O'Meara, O.T., *Introduction to Quadratic Forms*, Springer-Verlag, Berlin Heidelberg New York, 1973.

[7] Poonen, B., *Uniform first-order definitions in finitely generated fields*, December 2005. Preprint.

[8] Robinson, J., *The undecidability of algebraic rings and fields*, Proc. Amer. Math. Soc., 10 (1959), pp. 950-957.

[9] ———, *On the decision problem for algebraic rings*, Studies in Mathematical Analysis and Related Topics, no. 42, Stanford Univ. Press, Stanford, Calif., 1962, pp. 297–304.

[10] ———, *The decision problem for fields*, The Theory of Models: Proceedings of the 1963 International Symposium at Berkeley (J. W. Addison et al., eds.), North-Holland, Amsterdam, 1965, pp. 299–311.

[11] Robinson, R.M., *Intervals Containing Infinitely Many Set of Conjugate Algebraic Integers*, Studies in Mathematical Analysis and Related Topics, no. 43, Stanford Univ. Press, Stanford, Calif., 1962, pp. 305–315.

[12] Rumely, R.S., *Undecidability and definability for the theory of global fields*, Trans. Amer. Math. Soc. 262 (1980), no. 1, pp. 195–217.

[13] Siegel, C., *Approximation algebraischen Zahlen durch Quadrate*, Math. Z. 11 (1921), pp. 246–275.

[14] Swinnerton-Dyer. H.P.F., *A Brief Guide to Algebraic Number Theory*, London Mathematical Society Student Texts 50, Cambridge University Press, 2001.